شركات التجسس الصهيونية تعبّد طريق ابن سلمان إلى الحكم

تم الكشف عن تورط شركة كوا دريم الإسرائيلية في بيع أنظمة وأدوات تجسس لتعقب ناشطين في مؤسسات المجتمع المدني، وصحافيين ومعارضين في 10 دول مختلفة، بينها السعودية.

وبحسب ما تم الكشف استخدم برنامج تجسس وأدوات قرصنة من إنتاج شركة إسرائيلية في اختراق هواتف صحافيين ومعارضين ومنظمات حقوقية في 10 دول على الأقل.

بما في ذلك أشخاص بأميركا الشمالية وأوروبا وجنوب شرق آسيا وأوروبا والشرق الأوسط، بحسب ما جاء في تقريرين صدرا بالتوازي عن مختبر "سيتيزن لاب" المختص بالأمن الإلكتروني وشركة "مايكروسوفت".

وأفاد "سيتيزن لاب"، في تقرير، بأنه تمكن من التعرف على عدد قليل من ضحايا المجتمع المدني الذين تعرضت هواتفهم من طراز "آيفون" للاختراق باستخدام برنامج مراقبة طورته شركة "كوا دريم" (QuaDream) الإسرائيلية، وهي منافس أقل شهرة لشركة "إن إس أو" المتخصصة في برامج التجسس والتي أدرجتها الحكومة الأميركية في القائمة السوداء بسبب تورطها بالقرصنة على حقوقيين ومعارضين لأنظمة

استبدادية.

و"كوا دريم" هي واحدة من عدة شركات سيبرانية هجومية تعمل من إسرائيل، وتعمل في مجال تطوير أدوات اختراق لهواتف "آيفون" المخصصة لعملاء من الحكومات.

وبحسب المختبر المختص بالأمن السيبراني، فإن تعقب الخوادم التي تستخدمها "كوا دريم" إلى مشغليها، تظهر أن أدوات القرصنة استخدمت في بلغاريا، والتشيك، وهنغاريا، وغانا، وإسرائيل، والمكسيك، ورومانيا، وسنغافورة، والإمارات، وأوزبكستان.

وذكر "سيتيزن لاب"، أنه قام بتطوير أدوات "مكنته من تحديد ما لا يقل عن خمسة ضحايا من المجتمع المدني لبرامج التجسس والأدوات الخاصة لـ'كوا دريم'؛ من بين الضحايا صحافيون وشخصيات سياسية معارضة وعامل بمنظمة غير حكومية".

وأفاد بأنه "لن نقوم بتسمية الضحايا في هذه المرحلة". وقال إن أدوات قرصنة الشركة الإسرائيلية تعتمد على تقنية "click-zero" أو الهجوم بدون أي نقرات، ويستهدف نظام تشغيل iOS 14، بما في ذلك إصدارات iOS 14.4 و14.4.2، وربما الإصدارات الأخرى.

وقالت "مايكروسوفت"، في تقرير نُشر بالتزامن مع تقرير "سيتيزن لاب"، إنها تعتقد "بثقة عالية" أن برنامج التجسس "مرتبط بقوة بشركة كوا دريم".

وأفادت المسؤولة في شركة "مايكروسوفت"، آيمي هوجان بيرني، في بيان، إن مجموعات القرصنة المرتزقة مثل "كوا دريم" "تزدهر في الظل" وإن كشفها "ضروري لوقف هذا النشاط".

وبحسب "سيتيزن لاب"، أبرمت "كوا دريم" شراكة مع شركة قبرصية تسمى InReach، والتي دخلت معها حاليًا في نزاع قانوني. ولفت إلى أن "العديد من الأفراد الرئيسيين المرتبطين بكلتا الشركتين لديهم اتصالات سابقة مع مزود آخر لخدمات تجسس (Verint) بالإضافة إلى وكالات المخابرات الإسرائيلية".

وسوّقت "قوادريم" منتجاتها، في سنواتها الأولى، بواسطة شركة InReach، المسجلة كأحد مالكي الشركة. وهدف استخدام الشركة القبرصية إلى الالتفاف على إشراف وزارة الأمن الإسرائيلية على الصادرات الأمنية، إذ أن شركة قبرصية لا تخضع لإشراف كهذا وليست ملزمة بأن تسجل في وزارة الأمن كمصدرة منتجات أمنية.

وأسس ثلاثة إسرائيليين شركة "قوادريم"، في العام 2016، وهم غاي غيفاع ونيمرود رينسكي وإيلان دبلستين، والأخير كان ضابطا في شعبة الاستخبارات العسكرية الإسرائيلية. ويتولى آفي رابينوفيتش منصب مدير عام الشركة.

وأداة القرصنة التي طورتها "كوا دريم" تسمى "راين" (reign)، على غرار "بيغاسوس" لـ"إن إس أو"، والثغرة التي يستغلها برنامج التجسس في هذا الصدد، ويكشف عنها لأول مرة الآن، هي اختراق خدمة التقويم الرقمي التابعة لـ"آبل" – Calendar iCloud – ما يسمح للمهاجمين بإرسال استدعاء وهمي للهاتف وبالتالي الوصول إليه.

وتستعرض "كوا دريم" لزبائنها أداة الاختراق، Reign، وهي قادرة على اختراق أجهزة آيفون من دون حاجة إلى ضغط حامل الجهاز على أي رابط، بينما يحتاج حامل جهاز أندرويد إلى الضغط مرة واحدة على رابط يرسل إلى هاتفه.

وحسب المعلومات التي تزودها "كوا دريم" لزبائنها، فإنه بالإمكان استخراج أي معلومات بالإمكان تخيلها من الهاتف، وحتى معلومات لم تعد موجودة فيه، مثل سرقة أي نوع من الوثائق أو معلومات من الهاتف، وبينها صور، مقاطع فيديو، رسائل إلكترونية، رسائل واتسآب أو تيليغرام وما إلى ذلك، إضافة إلى تشغيل الكاميرا والميكروفون و GPS من أجل التجسس على حامل الهاتف.

وفي شباط/ فبراير 2022، قالت 5 مصادر تحدثت لوكالة "رويترز" إن شركة "كوا دريم" استغلّت ثغرة في برمجيات شركة "آبل" في الوقت ذاته الذي استطاعت فيه مجموعة "إن إس أو" الإسرائيلية للاستخبارات الإلكترونية اختراق هواتف آيفون في 2021.

واكتسبت الشركتان المتنافستان في 2021 القدرة على اختراق هواتف "آيفون" عن بُعد وفقًا لما قالته المصادر الخمسة لـ"رويترز"، وهو ما يعني أن بإمكان الشركتين تعريض هواتف شركة "آبل" للخطر دون أن يفتح أصحابها روابط خبيثة.

وقال خبير إن استخدام الشركتين الإسرائيليتين لأسلوب واحد متطور يعرف باسم "زيرو كليك"، يثبت أن الهواتف أكثر ضعفًا أمام أدوات التجسس الرقمي الفعالة مما تعترف به صناعة الهواتف.

ويعتقد خبراء يعكفون على تحليل اختراقات مجموعة "إن إس أو" وشركة "كوا دريم" منذ عام 2021، أن

الشركتين استخدمتا أساليب برمجية متشابهة جدًا تعرف باسم "فورسد إنتري" في اختراق هواتف آيفون.

وقال ثلاثة من المصادر إن المحللين أبدوا اعتقادهم أن أساليب الشركتين في الاختراق متشابهة لأنهما استغلتا ثغرات واحدة في منصة التراسل الفوري الخاصة بشركة "آبل" واستخدمتا أسلوبًا متشابهًا في زرع برمجيات خبيثة في الأجهزة المستهدفة.

وفي حزيران/ يونيو 2021، كشفت صحيفة "ذي ماركر" أن شركة "كوا دريم" تقدم خدمات سايبر هجومية للنظام السعودي، وهي واحدة من شركات السايبر الهجومية الإسرائيلية التي تعاقد معها النظام السعودي.

ونقلت الصحيفة عن مصدر قوله إنه "بين زبائن 'كوا دريم' أجهزة إنفاذ القانون وحكومات في عدة دول شرعية في الغرب، ولكن هناك آخرون".

وأضافت الصحيفة أن "كواد ريم" زودت خدماتها للحكومة السعودية منذ العام 2019، "وتكنولوجيتها معروفة لجهات أمنية تعتبر موالية لولي العهد السعودي، محمد بن سلمان، الذي تحول إلى الشخصية الأكثر تأثيرا في المملكة في السنوات الأخيرة، والمعروف عنه أنه لا يوفر أي وسيلة من أجل ترسيخ مكانته في المملكة".

وفي تموز/ يوليو 2021، كشفت صحيفة "نيويورك تايمز" الأميركية، أن وزارة الأمن الإسرائيلية، أصدرت تصاريح تصدير رسمية لأربع شركات تعمل في مجال البرمجة والهايتك الإسرائيلية من بينها شركة "كوا دريم"، لبيع برمجياتها الخاصة بالتجسس والقرصنة، للسلطات في السعودية.

وأفادت بأنه "منذ العام 2017 دخل إلى السعودية العشرات من الإسرائيليين الضالعين في الشأن الاستخباراتي، ومعظمهم من وحدات سيبرانية".

وقالت إن شركات السايبر الهجومي التي حصلت على تفويض للعمل مع السعودية هي "إن إس أو" و"كانديرو" و"فيرينت" و"كوا دريم"، وذكرت أن الشركتين الأخيرتين منحتا التفويض بعد مقتل الصحافي جمال خاشقجي.